



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,753	11/26/2003	Choon B. Shim	QOVI-002/00US	3938
7590 08/29/2007				
ATTN: Patent Group		EXAMINER		
COOLEY GODWARD LLP		TRAORE, FATOUMATA		
One Freedom Square, Reston Town Center				
11951 Freedom Drive		ART UNIT PAPER NUMBER		
Reston, VA 20190-5656		2136		
			MAIL DATE	DELIVERY MODE
			08/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/721,753

Applicant(s)

SHIM ET AL.

Examiner

Fatoumata Traore

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1022 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in response of the original filing of November 26th, 2003. Claims 1-22 are pending and have been considered below.

Claim Objections

2. Claims 1, 3, 6 are objected to because of the following informalities: regarding claim 1, line 4 "a" should be replace with "the", line 5 "a access" should be replace with "an access"; regarding claim 3, line 2 "the" should be inserted in front of "server"; regarding claim 6, line 2 "the" should be inserted in front of "first" and so on. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2, 7, 9, 11, 12 are rejected under 35 U.S.C. 102(e) as being anticipated by Nagaoka et al (US 6651174).

Claim 1: Nagaoka et al discloses a method for remotely controlling a network comprising:

- i. Configuring a first control unit inside a first firewall (column 7, lines 1-20 and FIG. 1);
- ii. Configuring a server outside the first firewall (column 7, lines 1-20 and FIG. 1); and
- iii. Establishing a session between the first control unit and the server, wherein establishing a session is executed using an access key (column 7, lines 1-20 and FIG. 1).

Claim 2: **Nagaoka et al** discloses a method for remotely controlling a network as in claim 1, and further discloses a step of configuring a second control unit inside a second firewall, the server being outside the second firewall (column 2, lines 2-20 FIG 1, FIG. 4).

Claim 7: **Nagaoka et al** discloses a method for remotely controlling a network as in claim 1 above, and further discloses a step of establishing a session between the first control unit and the server includes coupling through a second firewall, the server being inside the second firewall (column 6, lines 13-51).

Claims 9, 12: **Nagaoka et al** discloses a communication system comprising:

- iv. A first enterprise network (column 7, lines 1-20 and FIG. 1, FIG 5);
- v. A first control unit coupled to the first enterprise network (column 7, lines 1-20 and FIG. 1, FIG 5);

Art Unit: 2136

vi. A first firewall coupled to the first control unit (column 7, lines 1-20 and FIG. 1, FIG 5);

vii. A public network (FIG 5); and

viii. A server coupled to the public network, the first control unit being configured with server

information, the server being configured with first control unit information, the first control unit being further configured to send a first access key to the server, the first control unit and the, server configured to establish a communication session based on the first access key (FIG. 7A, FIG 7B).

Claim 11: **Nagaoka et al** discloses a communication system as in claim 9 above, and further comprising:

i. A second firewall coupled to the public network (column 7, lines 21-31 and FIG 1, FIG 2);

ii. A second control unit coupled to the second firewall (column 7, lines 21-31 and FIG 1, FIG 2); and

iii. A second enterprise network coupled to the second control unit, the second control unit

being configured with server information, the server being configured with second control unit information, the second control unit being further configured to send a second access key to the server, the second control

unit and the server configured to establish a communication session based on the second access key (FIG 7A, FIG 7B).

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 16, 18, 19, 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Crichton et al (US 6104716).

Claim 16: Crichton et al discloses a system for secure communication tunneling over the Internet comprising:

- i. A first console configured to generate at least one request (FIG. 5);
- ii. A proxy server coupled to the first console, the proxy server configured to pool the at least one request (FIG. 5);
- ii. A first firewall coupled to the proxy server (FIG. 3); and

iv. A first control unit coupled to the first firewall, the first control unit configured to receive the at least one request from the proxy server, the first control unit further configured to output at least one response corresponding to the at least one request to the proxy server, the proxy server configured to output the at least one response to the first console (column 5, lines 45-60, and FIGs. 3, 4, 5-8).

Claim 18: **Crichton et al** discloses a system for secure communication tunneling over the Internet as in claim 16 above, and further discloses:

A second firewall coupled to the proxy server (column 3, line 28 to column 6 line 9); and

A second control unit, the second control unit coupled to the second firewall, the second control unit configured to receive the at least one request from the proxy server, the second control unit further configured to output at least one response corresponding to the at least one request to the proxy server, the proxy server configured to output the at least one response to the first console (column 5 line 61 to column 6 line 38, column 10 lines 35-53FIG 5).

Claim 19: **Crichton et al** discloses a system for secure communication tunneling over the Internet as in claim 16 above, and further discloses:

i. A client request handler for receiving a client request from the first console (column 7, lines 10-15, and FIG 5);

- ii. A shared request object pool coupled to the client request handler, the shared request object pool configured to store the at least one request (column 8, lines 24-52, and FIG. 8); and
- iii. A server request handler coupled to the shared request object pool, the server request handler configured to read the at least one request from the shared request object pool, the server request handler configured to send the at least one request to the first control unit, the server request handler configured to receive the at least one response, the server request handler configured to output the at least one response to the first console (column 7, line 58 to column 8 line 23, and FIG 7).

Claim 21: **Crichton et al** discloses a system for secure communication tunneling over the Internet comprising:

- i. Receiving a request from a console (FIG. 8);
- ii. Creating a request object (FIG. 8);
- iii. Adding the request object to a pool (FIG. 8); and
- iv. Notifying a control unit of the request object (FIG. 8).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2136

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 3-6, 8, 10, 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nagaoka et al (US 651174) in view of Brownell (US 6754831).

Claim 3: Nagaoka et al discloses a method for remotely controlling a network as claim 1 above, which further discloses a step of receiving server identification information (FIG 3, FIG 4) and a step of sending the access key and the identification information to the server (FIG 3, FIG 4). Although it is clear that the teaching of Nagaoka et al inherently involve generating access key in the first control unit, Nagaoka et al was silent about the step generating access key during the authentication process. However, generating access key in the first control unit was known and commonly practiced in the art at the time the invention was made. Further as evidence by the teaching of Brownell a method of authentication firewall tunneling framework (column 11 line 30-65 and FIG. 4, block 430). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al such as to include the step of generating access key. One would have been motivated to do so in order to enable authentication between entities in communication.

Claims 4, 10: Nagaoka et al and Brownell disclose a method and system for remotely controlling a network as claims 3 and 9 above, and Brownell further

discloses that the step of receiving the server identification information includes receiving a server host name, a server IP address, and a server port number (column 8 line 54 to column 9 line 65, and FIG. 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of **Nagaoka et al** such as to add a step of receiving information. One would have been motivated to do so in order to enable authentication between entities in communication.

Claim 5: **Nagaoka et al** and **Brownell** disclose a method for remotely controlling a network as claim 3 above, and **Brownell** further discloses that the step of receiving the server identification information includes inquiring the server from the first control unit to obtain the server IP address (column 8 lines 28-51, and FIG. 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of **Nagaoka et al** such as to add a step of receiving information. One would have been motivated to do so in order to enable authentication between entities in communication.

Claims 6, 13: **Nagaoka et al** discloses a method and system for remotely controlling a network as claims 1 and 12 above, which further discloses a step of receiving first control unit identification information (FIG 3, FIG 4) and a step exchanging a validation message between the first control unit and the server (FIG 3, FIG 4). Although it is clear that the teaching of **Nagaoka et al** inherently

involve storing identification information and adding the control unit to the remote device, Nagaoka et al was silent about the step storing identification information and adding the control unit to the remote device. However, storing the first control unit identification information and adding the first control unit as a first remote device was known and commonly practiced in the art at the time the invention was made. Further as evidence by the teaching of Brownell a method of authentication firewall tunneling framework which further discloses a step of storing the first control unit identification information in the server (FIG. 2) and a step of adding the first control unit as a first remote device (FIG. 9) (column 11 line 30-65 and FIG. 4, block 430). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Nagaoka et al such as to include the step of generating access key. One would have been motivated to do so in order to enable authentication between entities in communication.

Claim 8: Nagaoka et al discloses a method for remotely controlling a network as claim 7 above, but does not explicitly describe the step of connecting between the server and a console. However, Brownell discloses a method of authentication firewall tunneling framework which further discloses a step of connecting between the server and a console the console being inside the second firewall, the connecting using an IP address facing inside the second firewall (column 4, lines 30-55, and FIG 1). Therefore it would have been

obvious for one of ordinary skill in the art at the time the invention was made to modify the teaching of **Nagaoka et al** such as to establish the connection between the server and a second firewall. One would have been motivated to do so in order to prevent attempts to gain access critical data.

Claim 14: **Nagaoka et al** and **Brownell** disclose a system for remotely controlling a network as claim 13 above, and **Nagaoka et al** further discloses:

- i. A second firewall coupled to the public network (column 7, lines 21-31 and FIG 1, FIG 2);
- ii. A second control unit coupled to the second firewall (column 7, lines 21-31 and FIG 1, FIG 2); and
- iii. A second enterprise network coupled to the second control unit, the second control unit being configured with server information, the server being configured with second control unit information, the second control unit being further configured to send a second access key to the server, the second control unit and the server configured to establish a communication session based on the second access key (FIG 7A, FIG 7B).

Claim 15: **Nagaoka et al** discloses a system for remotely controlling a network as claim 14 above, which further discloses a step of receiving first control unit identification information (FIG 3, FIG 4) and a step exchanging a validation

message between the first control unit and the server (FIG 3, FIG 4). Although it is clear that the teaching of **Nagaoka et al** inherently involve storing identification information and adding the control unit to the remote device, **Nagaoka et al** was silent about the step storing identification information and adding the control unit to the remote device. However, storing the first control unit identification information and adding the first control unit as a first remote device was known and commonly practiced in the art at the time the invention was made. Further as evidence by the teaching of **Brownell** a method of authentication firewall tunneling framework which further discloses a step of storing the first control unit identification information in the server (FIG. 2) and a step of adding the first control unit as a first remote device (FIG. 9) (column 11 line 30-65 and FIG. 4, block 430). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of **Nagaoka et al** such as to include the step of generating access key. One would have been motivated to do so in order to enable authentication between entities in communication.

8. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Crichton et al** (US 6104716) in view of **Nagaoka et al** (US 651174).

Claim 17: **Crichton et al** discloses a system for secure communication tunneling over the Internet as in claim 16 above, and further discloses but does not

explicitly discloses a second console coupled a proxy. However, Nagaoka et al discloses a system for remotely controlling a network, which further discloses a second console coupled to the proxy server, the second console configured to generate at least one other request, the proxy server configured to pool the at least one other request (FIG. 5, FIG. 7B). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Crichton et al such as to couple a second console with proxy (firewall). One would have been motivated to do so in order to present against unauthorized access.

9. Claims 20, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crichton et al (US 6104716) in view of Nelson (US 6553422).

Claim 20: Crichton et al discloses a system for secure communication tunneling over the Internet as in claim 16 above, but does not explicitly discloses the step of receiving, writing, reading a request and outputting a response. However, Nelson discloses a reserve http connection for device management, which further performs the steps of:

- b. Receiving a client request from the first console (column 4 line11-53, and FIG. 3, FIG. 4);
- c. Writing the at least one request (column 60-67);

Art Unit: 2136

- d. Reading the at least one request (column 4 line11-53, and FIG. 3, FIG. 4);
- e. Sending the at least one request to the first control unit column 4 line11-53, and FIG. 3, FIG. 4);
- f. Receiving the at least one response column 4 line11-53, and FIG. 3, FIG. 4); and
- g. Outputting the at least one response to the first console column 4 line11-53, and FIG. 3, FIG. 4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Crichton et al such as to read, send, and output a request. One would have been motivated to do so in order to present against unauthorized access.

Claim 22: Crichton et al discloses a system for secure communication tunneling over the Internet as in claim 21 above, but does not explicitly disclose the step of receiving, writing, reading a request and outputting a response. However, Nelson discloses a reserve http connection for device management, which further performs the steps of:

- a. Establishing a data connection with the control unit (column 4 line11-53, and FIG. 3, FIG. 4);
- b. Receiving a request from the control unit for the request object (column 4 line11-53, and FIG. 3, FIG. 4);

- c. Sending the request object to the control unit (column 4 line11-53, and FIG. 3, FIG. 4);
- d. Receiving a response from the control unit based on the request object (column 4 line11-53, and FIG. 3, FIG. 4); and
- e. Sending the response to the console (column 4 line11-53, and FIG. 3, FIG. 4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Crichton et al such as to read, send, and output a request. One would have been motivated to do so in order to present against unauthorized access.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Tanno US 63742298 System for performing remote operation between firewall equipped networks or devices.
- b. Cheng et al US 7107609 Stateful packet forwarding in a firewall cluster
- c. Wesinger et al US 6751738 Firewall providing enhanced network security and user transparency.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571)

Art Unit: 2136


270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Tuesday, August 28, 2007

Nassar G. Moazzami
Supervisory Patent Examiner


8,28,07